iSpirit 3524G/F 交换机常用配置指南

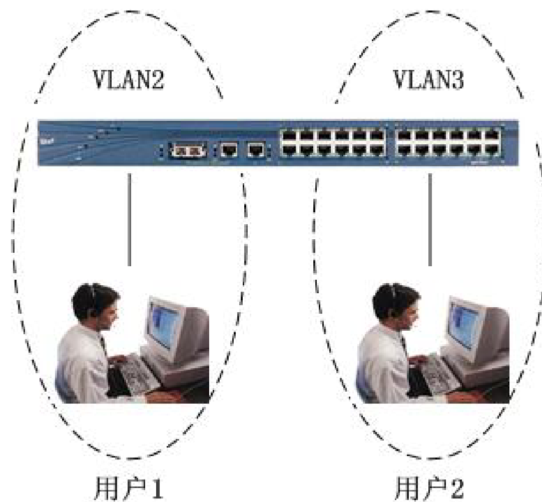
(软件版本：iSpirit3524g2v20.img iSpirit3524f2v00.img)

（Version 1.0）

2004 年 11 月



一．基于 PORT（端口）的 VLAN 配置



1．网络需求

有两个用户，用户 1 和用户 2，两个用户由于所使用的网络功能和环境不同，需要分别处于不同的 VLAN 中。用户 1 在 VLAN2，连接 3524G 的端口 2，用户 2 在 VLAN3，连接端口 3。

2．配置步骤

Switch# vlan 2　　// 创建 vlan 2
　Vlan 2 added
Switch(vlan-2)#exit
Switch# vlan 3　　// 创建 vlan 3
　Vlan 3 added
Switch(vlan-3)# vlan 2　　// 在创建 vlan 2 之后,就可在配置模式下 输入 vlan 2 ，进入 vlan 2 的配置模式
Switch(vlan-2)# untag 2　　// 将端口 2 加入 vlan 2,如果还有其它端口要加入 vlan 2，那么在 vlan 2 模式下，untag x （x 为其它端口号）

Switch(vlan-2)# vlan 3　　//进入 vlan 3 配置模式
Switch(vlan-3)# untag 3　　//将端口 3 加入 vlan 3，如果还有其它端口要加入 vlan 3，那么在 vlan 3 模式下，untag x （x 为其它端口号）

Switch(vlan-3)# exit

// 注意：本例子中，由于使用的软件版本是 2v.00 以上（含 2v.00）,所以 pvid 号随着 vlan 号的更改而自动更改的。不用手工设置。
对于较早版本（2v.00 版以前）的交换机，需要设置 pvid 号，pvid 号与端口所在

的 vlan 号一样。例如：本案例中假如是采用低于 2v.00 版的软件，那么就要进行下面的相关设置。

Switch# port 2 // 进入端口 2
Switch(port-2)# pvid 2 //设置端口 2 的 pvid 号为 2

Switch(port-2)# port 3 // 进入端口 3
Switch(port-3)# pvid 3 //设置端口 3 的 pvid 号为 3

3. 排错 ：

如果配置后，发现不同 VLAN 之间的 PC 机不能通信，那是正常现象，因为不同 VLAN 之间要进行通信，必须要经过三层的路由转发。

如果同一 VLAN 内的 PC 机不能进行通信，须作以下验证：

1）查看整体有哪些 VLAN

Switch# show vlan

```
-----------------------------------------------
|VID |Name                              | Status |
|----+--------------------------------+--------|
|1    |Default VLAN 1                  | Static |
|---------------------------------------------|
|2    |vlan2                            | Static |
|---------------------------------------------|
|3    |vlan3                            | Static |
|---------------------------------------------|
```

// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，(VID 号为 2 和 3) 就要重新配置。

注意：这里关键要看 VID 下面说对应的值，Name 仅仅是个名字标识，没什么大关系。

2） 看设置的端口是否在相应的 VLAN 内，并且是以 " U " 的形势加入的

Switch# show vlan 2 //查看 vlan 2 的配置

```
Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                        (-=None, M=Member, F=Forbidden, U=Untagged)
-------------------------------------------------------------------
|  Port Number   |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|                |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
```

// 查看 vlan 2 ，发现端口 2 标记为 “U”，说明配置正确。 如果 U 不是标记在 2 处，那么就是配置有问题，要重新配置

Switch# show vlan 3 //查看 vlan 3 的配置

```
Vlan ID:          3
Vlan Name:        vlan3
Vlan Status:      Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
-------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-------------------------------------------------------------------
```

// 查看 vlan 3 ，发现端口 3 标记为 “U”，说明配置正确。如果 U 不是标记在 3 处，那么就是配置有问题，要重新配置

3） 查看特定端口，端口的 pvid 号必须和端口所在 vlan 的号码一致

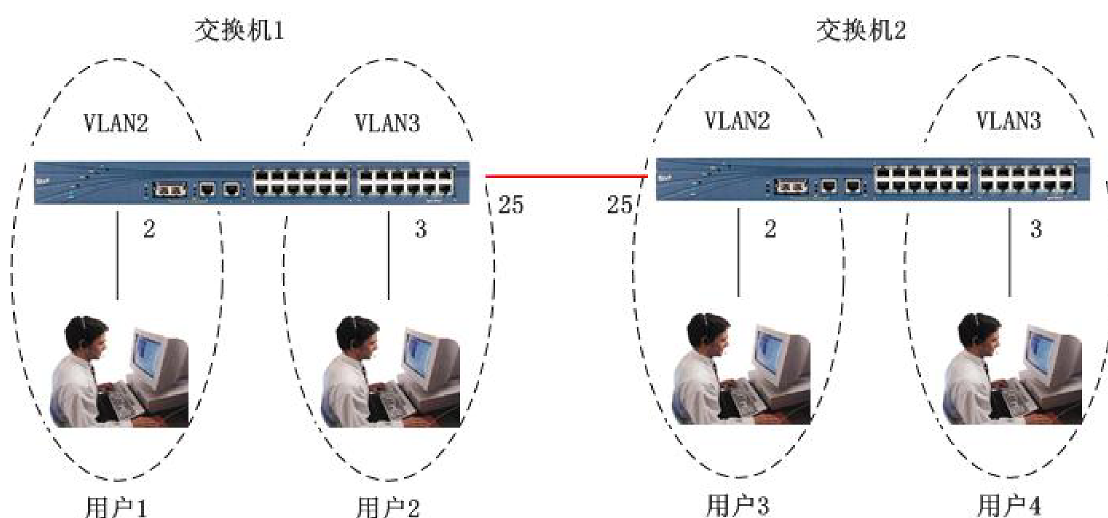
如例，端口 2 在 vlan 2 中，端口 2 的 pvid 号应该为 2 。

```
Switch# show port 2
 Unit                 :  1
 Port                 :  2
 ifIndex              :  0x2100002
 State                :  Enable
 Set Speed            :  autonegotiate
 Actual Speed         :  unknown
 STP State            :  Disabled
 Link                 :  Down
 MacLearn             :  Unlock
 PortVlanID           :  2     // 端口 2 的 pvid 号为 2 ，配置正确
 PortDefaultPriority :  0
 DropEvents           :  0

Switch# show port 3
 Unit                 :  1
 Port                 :  3
 ifIndex              :  0x2100003
 State                :  Enable
```

Set Speed : autonegotiate
Actual Speed : unknown
STP State : Disabled
Link : Down
MacLearn : Unlock
PortVlanID : 3 //端口 3 的 pvid 号为 3，配置正确
PortDefaultPriority : 0
DropEvents : 0

二．基于 802.1Q 的 vlan 配置



1.网络需求 ：

有两台 3524G 交换机分别连接两个用户。用户 1 和 3 属于 vlan 2，用户 2，4 属于 vlan 3。详细情况如下：

用户	所属 VLAN	连接端口	所属交换机	级联端口
用户 1	Vlan2	2	交换机 1	25
用户 2	Vlan3	3	交换机 1	
用户 3	Vlan2	2	交换机 2	25
用户 4	Vlan3	3	交换机 2	

2．配置步骤：

交换机 1：

witch# vlan 2
 Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit

Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit

// 注意：本例子中，由于使用的软件版本是 2v.00 以上（含 2v.00），所以 pvid 号随着 vlan 号的更改而自动更改的。不用手工设置。

对于较早版本（2v.00 版以前）的交换机，需要设置 pvid 号，pvid 号与端口所在的 vlan 号一样。例如：本案例中假如是采用低于 2v.00 版的软件，那么就要进行下面的相关设置。

Switch# port 2 // 进入端口 2
Switch(port-2)# pvid 2 //设置端口 2 的 pvid 号为 2

Switch(port-2)# port 3 // 进入端口 3
Switch(port-3)# pvid 3 //设置端口 3 的 pvid 号为 3

在本案例中，端口 25 既属于 vlan2，也属于 vlan3，它是一个标记为 tagged 的端口，所以不用设置它的 pvid 号，让它保持默认值：Pvid=1。

交换机 2：

witch# vlan 2
 Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit

Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit
Switch# port 2



有关 pvid 的相关说明，请见本例中交换机 1 的注意部分。

3．排错：

跨交换机的 vlan，在同一个 vlan 内的 pc 机都能够通信的，如果不能通信，需要查看的信息如下：

1、 连接 pc 机的端口是以"u"模式加入这个 vlan 的，并且端口的 pvid 号和 vlan 号应该一致
2、 级联端口是加入到每一个 vlan 中的，并且在每一个 vlan 内都是以"M"模式加入的，并且端口的 pvid 号为 1。

查看交换机 1 的配置

Switch# show vlan //查看整体 vlan 的配置

```
-----------------------------------------------
|VID |Name                          | Status |
|----+------------------------------+--------|
|1   |Default VLAN 1                | Static |
|--------------------------------------------|
|2   |vlan2                         | Static |
|--------------------------------------------|
|3   |vlan3                         | Static |
|--------------------------------------------|
```

Switch# show vlan 2 //查看 vlan 2 的配置

```
Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                         (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|M|-|
--------------------------------------------------------------------
```

// 查看 vlan 2 ，发现端口 2 标记为 "U"，端口 25 标记为 "M"， 说明配置正确。 如果 U 不是标记在 2 处，那么就是配置有问题，要重新配置

Switch# show vlan 3 //查看 vlan 3 的配置

Vlan ID: 3
Vlan Name: vlan3
Vlan Status: Static

(-=None, M=Member, F=Forbidden, U=Untagged)

```
 ---------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|M|-|
 ---------------------------------------------------------------------
```

注意交换机的端口 2 的 pvid 号为 2，端口 3 的 pvid 号为 3，级联端口 25 的 pvid 还是为 1。查看端口状态（包行 pvid 信息）的命令为：swtich# show port x （x 为端口号）。

查看交换机 2 的配置

由于在本案例中，交换机 2 的配置和 交换机 1 的配置是一样的，所以查看配置方法和结果应该是一样的。如果不一样，就要重新配置一下。

三．vlan 间通信配置

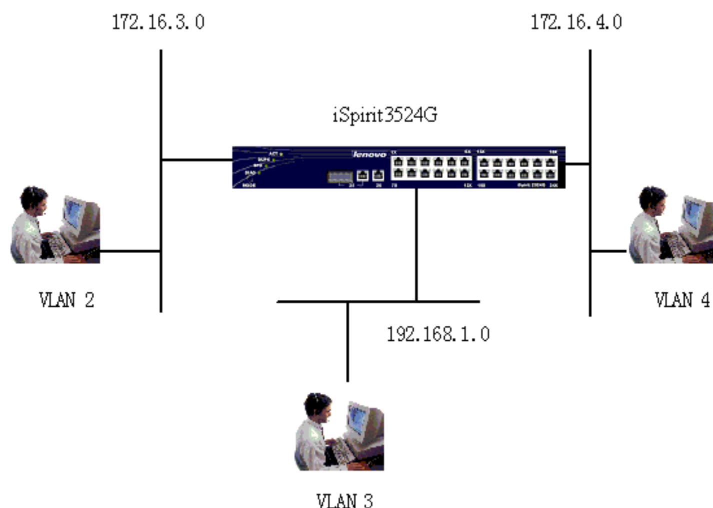
1.vlan 间通信配置实例一

1.1 网络需求

某公司采用 iSpirit3524G 构建局域网。为了使公司的局域网达到一个较好的效果，在 iSpirit 3524G 上划分三个 vlan，并启用三层转发，实现 vlan 间通信。

具体要求如下：
vlan 2（端口 1—2)、vlan 3（端口 3—4)、vlan 4（端口 5—6)，
vlan 2 的子网接口为 172.16.3.1 子网掩码：255.255.255.0
vlan 3 的子网接口为 192.168.1.1 子网掩码：255.255.255.0
vlan 4 的子网接口为 172.16.4.1 子网掩码：255.255.255.0

拓扑图如下：



1.2 配置步骤

1).在 35 交换机上配置三个 vlan ：vlan2 vlan 3 vlan 4

```
Switch# vlan 2
  Vlan 2 added
Switch(vlan-2)#untag 1-2
Switch(vlan-2)#exit

Switch# vlan 3
  Vlan 3 added
Switch(vlan-3)#untag 3-4
Switch(vlan-3)# exit

Switch# vlan 4
  Vlan 4 added
Switch(vlan-4)#untag 5-6
Switch(vlan-3)# exit
```

2) 查看 vlan 的配置信息

```
Switch# show vlan
-----------------------------------------------
|VID |Name                           | Status |
|----+-------------------------------+--------|
|1   |Default VLAN 1                 | Static |
|---------------------------------------------|
|2   |vlan2                          | Static |
|---------------------------------------------|
|3   |vlan3                          | Static |
|---------------------------------------------|
|4   |vlan4                          | Static |
```

```
|---------------------------------------------|
```

3）查看每个 vlan 里的端口是否正确

```
Switch# show vlan 2

Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
---------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |U|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
---------------------------------------------------------------------

Switch# show vlan 3

Vlan ID:        3
Vlan Name:      vlan3
Vlan Status:    Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
---------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
---------------------------------------------------------------------

Switch# show vlan 4

Vlan ID:        4
Vlan Name:      vlan4
Vlan Status:    Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
---------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|-|-|U|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
---------------------------------------------------------------------
```

4）配置交换机的子网

```
Switch# route
```

```
Switch(route-config)# ip sub
Netware Interface: 2
Agent Ip Addr: 172.16.3.1
Net Mask: 255.255.255.0
Vlan ID: 2
Interface Descript: vlan2
Switch(route-config)# ip sub
Netware Interface: 3
Agent Ip Addr: 192.168.1.1
Net Mask: 255.255.255.0
Vlan ID: 3
Interface Descript: vlan3
Switch(route-config)# ip sub
Netware Interface: 4
Agent Ip Addr: 172.16.4.1
Net Mask: 255.255.255.0
Vlan ID: 4
Interface Descript: vlan4
```

5）查看配置子网的结果

```
Switch(route-config)# show ip sub ta

ifIndex  IP Address       NetMask          Vid Status    Desc
01100002 172.16.3.1       255.255.255.0      2 Active    vlan2
01100001 192.168.0.1      255.255.255.0      1 Active    Default IP Addr
01100003 192.168.1.1      255.255.255.0      3 Active    vlan3
01100004 172.16.4.1       255.255.255.0      4 Active    vlan4
```

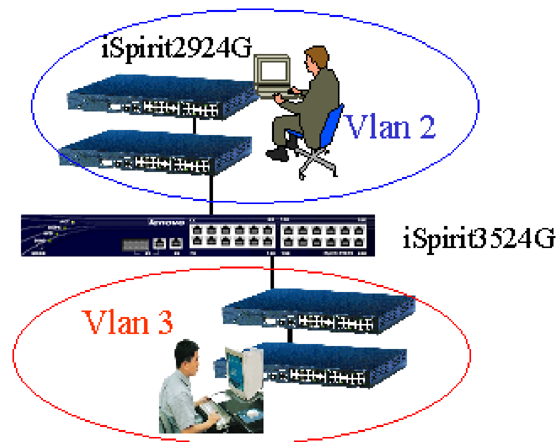
2.vlan 间通信配置实例二

2.1 网络需求

某公司采用 iSpirit3524G 和 iSpirit2924G 构建局域网。为了使公司的局域网达到一个较好的效果，在 iSpirit 3524G 上划分 2 个 vlan，并启用三层转发，实现 vlan 间通信。

具体要求如下：
vlan 2 (端口 2)、vlan 3 (端口 3)；
vlan 2 的子网接口为 172.16.2.1　子网掩码：255.255.255.0
vlan 3 的子网接口为 192.168.3.1　子网掩码：255.255.255.0
端口 2 和 端口 3 都接了 iSpirit 2924G

拓扑图如下：



2.2 配置步骤

1).在 35 交换机上配置三个 vlan ：vlan2 vlan 3

Switch# vlan 2
 Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)#exit

Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)#untag 3
Switch(vlan-3)# exit

2) 查看 vlan 的配置信息
Switch# show vlan

```
-----------------------------------------------
|VID |Name                              | Status |
|----+----------------------------------+--------|
|1   |Default                           | Static |
|------------------------------------------------|
|2   |vlan2                             | Static |
|------------------------------------------------|
|3   |vlan3                             | Static |
|------------------------------------------------|
```

3) 查看每个 vlan 里的端口是否正确
Switch# show vlan 2

```
Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
--------------------------------------------------------------------

Switch# show vlan 3

Vlan ID:        3
Vlan Name:      vlan3
Vlan Status:    Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
--------------------------------------------------------------------
```

4）配置交换机的子网

```
Switch(route-config)# ip sub
Netware Interface: 2
Agent Ip Addr: 172.16.2.1
Net Mask: 255.255.255.0
Vlan ID: 2
Interface Descript: vlan2
Switch(route-config)# ip sub
Netware Interface: 3
Agent Ip Addr: 192.168.3.1
Net Mask: 255.255.255.0
Vlan ID: 3
Interface Descript: vlan3
```

5）查看配置子网的结果

```
Switch# route
Switch(route-config)# show ip sub ta

ifIndex  IP Address      NetMask          Vid Status   Desc
```

```
01100002 172.16.2.1      255.255.255.0      2 Active    vlan2
01100001 192.168.0.1     255.255.255.0      1 Active    Default IP Addr
01100003 192.168.3.1     255.255.255.0      3 Active    vlan3
```

6) iSpirit2924G 的交换机可以不用配置

3.vlan 间通信配置实例三

3.1 网络需求

某公司采用 iSpirit3524G 和 iSpirit2924G 构建局域网。为了使公司的局域网达到一个较好的效果，在 iSpirit 3524G 上划分 2 个 vlan，并启用三层转发，实现 vlan 间通信。在 iSpirit 3524G 上划分 2 个 vlan,并启用三层转发,实现 vlan 间通信。同时,iSpirit2924G 也都划分了 2 个 vlan。

具体需求：
iSpirit3524
vlan 2（端口 1，14)、vlan 3（端口 1,14)；注意：vlan 2 和 vlan 3 所包含的端口都有端口 1，14，这是因为要使端口 1 属于 vlan 2 和 vlan 3，端口 14 也属于 vlan 2 和 vlan 3。端口 1 和 14 都是要标记为 tagged，只有打 tagged 标记的端口才可以属于多个 vlan。

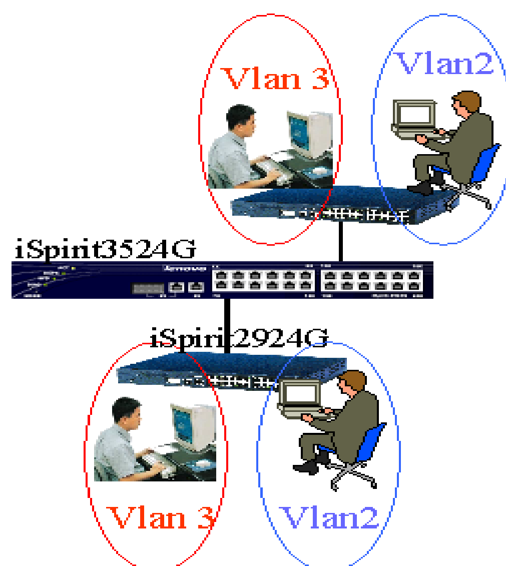
vlan 2 的子网接口为 172.16.2.1 子网掩码：255.255.255.0
vlan 3 的子网接口为 192.168.3.1 子网掩码：255.255.255.0

端口 1 和 端口 14 都接了 iSpirit 2924G；

两台 iSpirit2924G 上也都划分了 vlan2 和 vlan3；
vlan 2（端口 2-12)
vlan 3（端口 13-24)

其中,第一台 iSpirit 2924G 的第 1 端口连接到 iSpirit3524G 的第 1 端口,第二台 iSpirit 2924G 的第 1 端口连接到 iSpirit3524G 的第 14 端口。

拓扑图如下：



3．2 配置步骤

1).在 35 交换机上配置三个 vlan ：vlan2 vlan 3

```
Switch# vlan 2
  Vlan 2 added
Switch(vlan-2)# tag 1
Switch(vlan-2)# tag 14
Switch(vlan-2)#exit

Switch# vlan 3
  Vlan 3 added
Switch(vlan-3)# tag 1
Switch(vlan-2)# tag 14
Switch(vlan-3)# exit
```

2) 查看 vlan 的配置信息

```
Switch# show vlan

 -----------------------------------------------
|VID |Name                              | Status |
|----+----------------------------------+--------|
|1   |Default                           | Static |
|-----------------------------------------------|
|2   |vlan2                             | Static |
|-----------------------------------------------|
|3   |vlan3                             | Static |
```

```
|----------------------------------------------|
```

3）查看每个 vlan 里的端口是否正确

```
Switch# show vlan 2

Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                         (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |M|-|-|-|-|-|-|-|-|-|-|-|-|M|-|-|-|-|-|-|-|-|-|-|-|-|
```

```
Switch# show vlan 3

Vlan ID:        3
Vlan Name:      vlan3
Vlan Status:    Static
                         (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |M|-|-|-|-|-|-|-|-|-|-|-|-|M|-|-|-|-|-|-|-|-|-|-|-|-|
--------------------------------------------------------------------
```

4）配置交换机的子网

```
Switch(route-config)# ip sub
Netware Interface: 2
Agent Ip Addr: 172.16.2.1
Net Mask: 255.255.255.0
Vlan ID: 2
Interface Descript: vlan2
Switch(route-config)# ip sub
Netware Interface: 3
Agent Ip Addr: 192.168.3.1
Net Mask: 255.255.255.0
Vlan ID: 3
Interface Descript: vlan3
```

5）查看配置子网的结果

```
Switch# route
Switch(route-config)# show ip sub ta

ifIndex  IP Address      NetMask          Vid Status   Desc
01100002 172.16.2.1      255.255.255.0      2 Active   vlan2
01100001 192.168.0.1     255.255.255.0      1 Active   Default IP Addr
01100003 192.168.3.1     255.255.255.0      3 Active   vlan3
```

6）在 iSpirit2924 上配置两个 vlan（两台 iSpirit2924 配置相同）

```
Switch# vlan 2
 Vlan 2 added
Switch(vlan-2)# tag 1
Switch(vlan-2)#untag 2-12
Switch(vlan-2)#exit

Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)# tag 1
Switch(vlan-2)# untag 13-24
Switch(vlan-3)# exit
```

7）查看 vlan 的配置信息

```
Switch# show vlan

-----------------------------------------------
|VID |Name                           | Status |
|----+-------------------------------+--------|
|1   |Default                        | Static |
|---------------------------------------------|
|2   |vlan2                          | Static |
|---------------------------------------------|
|3   |vlan3                          | Static |
|---------------------------------------------|
```

8）查看每个 vlan 里的端口是否正确

```
Switch# show vlan 2

Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
```

```
                          (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number   |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|                |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|----------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration  |M|U|U|U|U|U|U|U|U|U|U|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
```

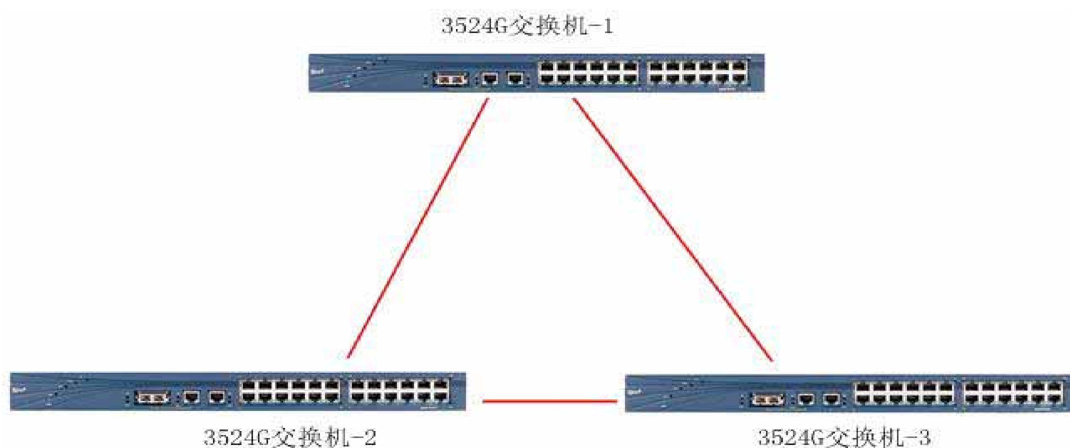
```
Switch# show vlan 3

Vlan ID:        3
Vlan Name:      vlan3
Vlan Status:    Static
                          (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
|  Port Number   |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|                |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|----------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration  |M|-|-|-|-|-|-|-|-|-|-|-|U|U|U|U|U|U|U|U|U|U|U|U|-|-|
```

四．STP（生成树协议配置）

1．网络需求：

为了避免三台 iSpirit3524G 连接在一起构成环路，需要配置 STP（生成树协议）。



2.配置步骤：

2.1 启用 stp

三台交换机连接成一个环状，需要打开每一台交换机的生成树协议，分别在每一台交换机上执行

```
Switch# stp enable    // 打开 stp 生成树协议
```

确认生成树协议在每一台交换机上是打开的

```
Switch# show switch
 Ip Address          : 192.168.0.1
 Subnet Mask         : 255.255.255.0
 Default Gateway     : 0.0.0.0
 MAC Address         : 00:09:ca:01:75:02
 BOOTP               : Disable
 DHCP                : Disable
 Spanning Tree       : Enable    //stp 已启用
 Traffic Classes     : Enable
 IGMP Snooping       : Enable
 Reset               : no reset
 DhcpRelay           : Disable
```

// 见到上述 stp 启用的信息，就说明生成树协议能正常运行。在默认情况下，每个端口都已经设置为参与 stp。所以在交换机全局模式下启用 stp，各端口也就能正常允许 stp。

如果需要关闭生成树协议的运行，需要输入命令

```
Switch# stp disable
```

2.2 生成树协议的高级命令：

设置第一台交换机为根交换机，需要设置他的桥优先级比其他两个桥的优先级要小，默认优先级为 32768

```
Switch# stp bridge priority  A        stp bridge priority (0=<A<=65535)
```

如果要使交换机的某个端口不参与生成树的运行，需要关闭端口的生成树功能

```
Switch# disable stp ports  A-B or A     port list (1=<A,B<=8)
```

在本案例中，不需要设置某些端口不参与生成树，所以不需要使用此命令。在默认情况下，iSpirit3500 系列的交换机的所有端口，都是参与生成树

3.排错：

3.1 查看哪一个交换机被选为根网桥：

```
Switch# show stp bridge
 --- Designated Root Information ---
 Priority                  : 32768
 MAC Address             : 00:09:ca:01:75:02          (根网桥配置状态)
 Hello Time                : 2s
 Forward Delay             : 15s
 Max Age                  : 20s

 --- Bridge STP Information ---
 Bridge Priority           : 32768
 MAC Address            : 00:09:ca:01:75:02          (本网桥配置状态)
 Root Path Cost            : 0
 Root Port                 : 0
 Bridge Hello Time         : 2s
 Bridge Forward Delay      : 15s
 Bridge Max Age           : 20s
```

3.2 查看生成树中交换机的端口状态：

```
Switch# show stp port   A     port number (1=<A<=8)

Switch# show stp port 1
 --- Port Information ---
 STP Port                  : Enable
 Port ID                   : 1
 Priority                  : 128
 State                     : Disabled
 Path Cost                 : 19
 Designated Cost           : 0

 --- Designated Root Information ---
 Priority                  : 32768
 MAC Address               : 00:09:ca:01:75:02

 --- Designated Port Information ---
 Port ID                   : 1
 Priority                  : 128
```

```
--- Designated Bridge Information ---
Priority                  : 32768
MAC Address               : 00:09:ca:01:75:02
```

四．Trunk 端口聚合

1.网络需求：

为了增加两台 iSpirit3524G 连接间的带宽，同时提供冗余功能，保证其中一条链路出了问题时，其它链路都可以正常使用，因此，在这里使用了 trunk 配置。

在交换机 1 和交换机 2 之间做 trunk 链路，各自捆绑 1-4 端口做链路聚合。



2.配置步骤：

在每个交换机上执行：

Switch# trunk <cr> set trunk configuration

Switch# trunk

trunk_Id: 1 // trunk 的 ID 号，ID 号范围：0-5

trunk_Rtag: 1 //trunk 的 tag 号，tag 号范围：1-6

ports_list: 1-4 //加入 trunk 组的端口号

注意:做 trunk 时，两边交换机的端口数量要一致，速度、双工等端口参数都要完全一致，但不必两边的端口号一一对应。iSpirit3524G/F 最多支持 6 组 trunk，每组 trunk 最多可以包含 8 个 100M 端口，或者 2 个 1000M 端口。

3．Trunk 删除命令：

删除一个 trunk 组

Switch# no trunk A trunk indentifier(0<=tid<=5)

删除所有的 trunk 组
Switch# trunk table init <cr>

4.排错

1） 如果 trunk 没有起作用，需要查看以下状态，检查所配置的 trunk 是否激活，包含的端口数量和端口号是否正确。

Switch# show trun

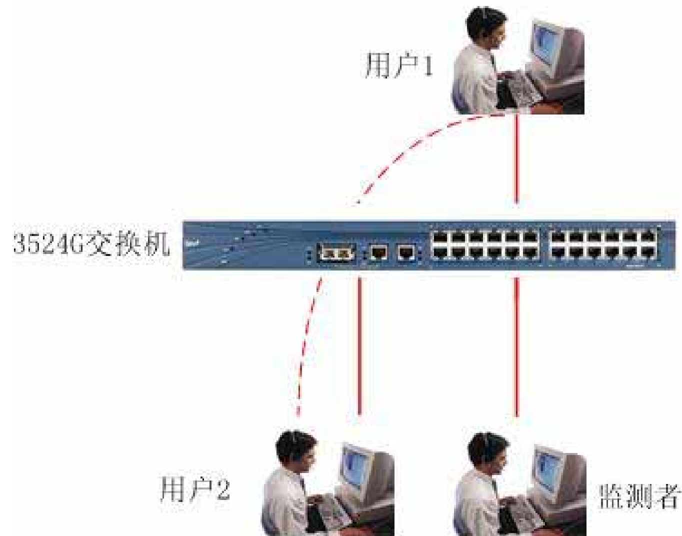
TGID	RTAG	status	Ports
0	0	Not_ready	0x00000000(none)
1	**1**	**Active**	**0x0000001e(fe1-fe4)**
2	0	Not_ready	0x00000000(none)
3	0	Not_ready	0x00000000(none)
4	0	Not_ready	0x00000000(none)
5	0	Not_ready	0x00000000(none)

2） 加入 trunk 组的几个端口一定要属于同一个 vlan，速率，双工等端口属性都要设置一样。

五. mirror （端口镜像）配置

1.网络需求：

在一台交换机中，用户 1 和用户 2 正在通信，正常情况下其他端口的用户是无法获取其通信信息的，为了检测数据流是否正常，监测者需要获取其数据流，就要用到端口镜像问题。用户 1 连接到端口 1，用户 2 连接到端口 2，监测者连接在端口 8，使监测者能够捕捉到其数据流。



2.配置：

2.1 监测用户 1 的流量

Switch# mirror
Mirror Mode: L2
Mirror Port: 8　　//监控者的端口
Egress ports_list: 1　　//被监控者出口流量的端口
Ingress ports_list: 1　　//被监控者入口流量的端口

2.2 监测用户 2 的流量

Switch# mirror
Mirror Mode: L2
Mirror Port: 8　　//监控者的端口
Egress ports_list: 2　　//被监控者出口流量的端口
Ingress ports_list: 2　//被监控者入口流量的端口

3.排错：

1) 不要把镜像端口和被镜像端口搞反了。
镜像端口是 mirror ports,指的是观测者所在的端口
被镜像端口是 Egress ports（外出数据流），Ingress ports （进入数据流），指的是被观测的端口

2) 用 show mirror 命令进行确认
mirror mode l2，指的是在二层的数据链路层上进行数据镜像的。

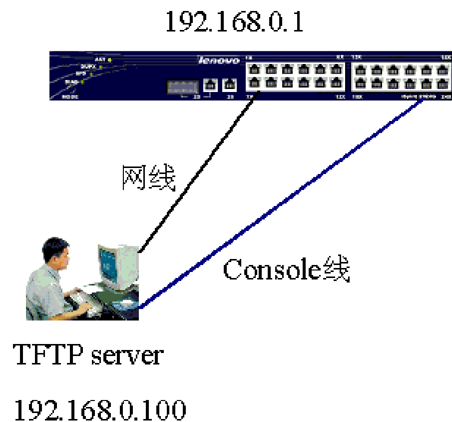
Switch# show mirror
Mirror Mode: L2
Mirror Port: 8
Egress ports_list: 1
Ingress ports_list: 1

六．Configuration 文件上传（备份）和下载配置

1．需求

1) 把交换机的配置文件上传（备份）到 TFTP 服务器上；
2) 把存放到 TFTP 服务器上的配置文件下载到交换机

网络拓扑图如下：



2．操作步骤

1) 设置 TFTP 服务器的 IP 地址为 192.168.0.1　3524G 交换机的 IP 地址为 192.168.1.100,并确保 TFTP 和交换机的 IP 之间能够相通

交换机 ip 地址的配置如下：

switch>enable

switch#ip add 192.168.0.1 255.255.255.0

2) 在 pc 上打开 TFTP 服务器

3) 把交换机的配置文件上传（备份）到 TFTP 服务器上,具体操作如下，在交换机上执行

Switch# upload configuration 192.168.0.100 文件名

uploading configuration ......

4) 如果为了方便，不想重新配置交换机，那么可以把保存在 TFTP 服务器上的配置文件向下传到交换机上，具体操作如下，在交换机上执行

Switch# download configuration 192.168.0.100 文件名

Do you wish to continue? [Y/N]: y

3.排错

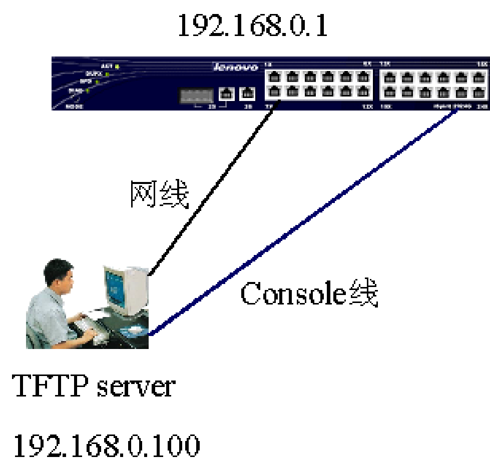
如果上传或者下载文件不成功，需要注意以下几个方面：

1) tftp 服务器和交换机之间的 IP 是一定要相互能通。
2) tftp 服务器的 tftp 服务一定要打开。
3) 在交换机上执行的下传或下载配置文件的命令一定要写正确，特别是配置文件的名字一定要正确，区分大小写。
4) 准备好的配置文件一定要放置到 tftp 服务器指定的目录下。

七．IMAGE 版本升级

1．网络环境：

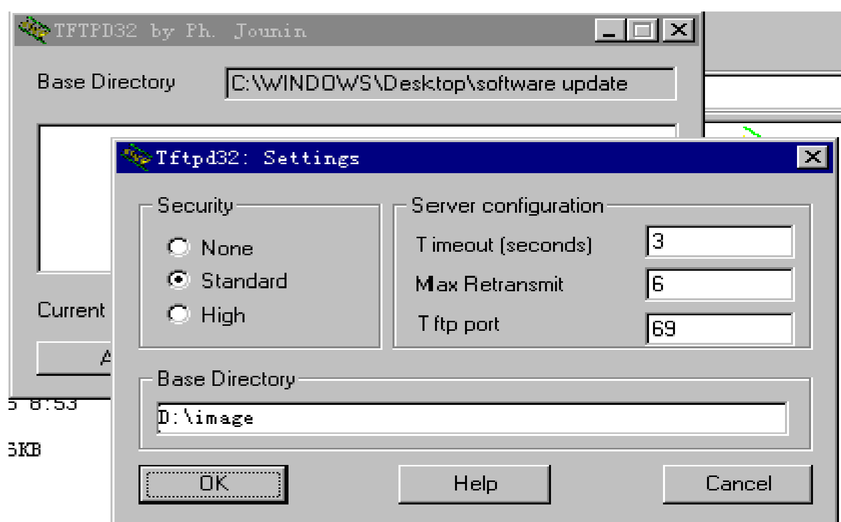
硬件：交换机，计算机，串口线，网线。
软件：windowns 操作系统，TFTP 服务器软件（tftpd32.exe 或者其它 tftp 软件）



2．配置步骤：

1) 配置交换机的 ip 地址
Switch>enable
Switch#ip add 192.168.0.1 255.255.255.0
Switch#show switch　//可以看到刚才配置的 ip 地址

2) 设置 pc 机的 ip 地址为 192.168.0.100 ，并运行 tftp 软件。



上　　述
D:\image 为升级文件所在的位置（即升级文件存放在 D：\image 目录下），可以根据实际情况进行设置。

3) 在超级终端下，输入 download 命令，开始下载镜像文件。

```
Switch# download image 192.168.0.100 ispirit2924g2v00.img
  Do you wish to continue? [Y/N]: y
  Don't Shut down power until completed!
  downloading image ......
```

一直等到交换机提示升级完成，然后才能重新启动交换机

注意：在升级交换机的过程中，不能断电。如果中途断电，很可能造成交换机损坏。

3．排错：

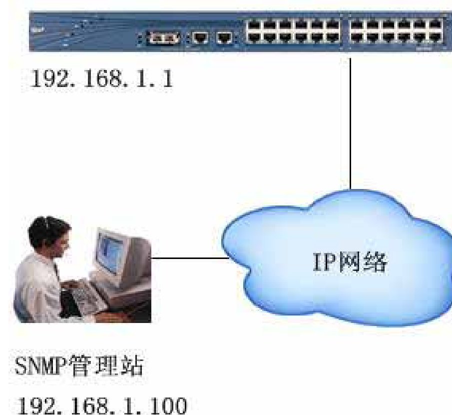
交换机映像文件升级不成功，需要查找以下几个原因：
1) 交换机和 TFTP 服务器之间是否 IP 能够通信。
2) TFTP 服务器是否正常启动，并且启动所用的 IP 地址就是交换机所能够 PING 通的。
3) 映像文件是否放到了 TFTP 服务器所指定的特定位置。
4) 在交换机上执行升级映像文件时，映像文件的名字一定不要写错。

八．snmp 配置

1.网络需求

有一个 SNMP 管理站上面运行 SNMP 管理软件，管理站的 IP 地址为 192.168.1.100。

现在，管理站要管理其中一台 IP 地址为 192.168.1.1 的交换机。由于该工作站有两个管理者，一个管理者只有对交换机有查看信息的权限，另一个管理者可以对交换机进行设置。因此。在交换机上打开 SNMP 后（默认是打开的），配置了 snmp 的 community ，一个为只读，另外一个为读写。其中，只读的 community 设置为 public，读写的 community 设置为 private。



2. 配置

1） 默认情况下，iSpirit3500 系列交换机已经启动了 snmp ，所以设置 snmp 时，只要设置 snmp community 和相关参数就可以。

Switch# snmp community
Community Name : public
//设置 community 为 public，这个参数是一个字符串，内容不限
View Name(internet) :
 ReadOnly(1),ReadWrite(2)
Permission : 1 //选择 1，将属性设置为只读

Switch# snmp community
Community Name : private
//设置 community 为 private，这个参数是一个字符串，内容不限
View Name(internet) :
 ReadOnly(1),ReadWrite(2)
Permission : 2 //选择 2，将属性设置为为读写。

查看 snmp community 的配置
Switch# show snmp community

CommunityName	ViewName	Permission	Status
public	internet	ReadOnly	Active
private	internet	ReadWrite	Active

如果查看到上述的配置信息。一般就没有问题了。接着就是对管理站进行相关设置。管理站的设置，请查阅管理软件的相关配置手册。

2) 配置了 snmp 之后，还可以进行可选配置，如 trap

trap 指的是当交换机发生特殊情况时，主动向 snmp 管理站发送 snmp 信息。

需要配置 trap 功能，选择 snmp 版本为 2

```
Switch# snmp trap
trap name : test
Target Ip Addr: 192.168.1.100
 snmpv1(1),snmpv2(2),snmpv3(3)
Version : 2
```

查看配置信息：

```
Switch# show snmp trap
--------------------------------------------------------------
 Trap Name            : test
 Transport Domain : 1.3.6.1.6.1.1
 Target ip            : 192.168.1.100
 Target port          : 162
 TimeOut              : 1500
 Retry Count          : 0
 Tag List             : rfc1493 rfc1757 rfc1907 rfc2233 tmscom
 Version              : snmp V2
 Storage Type         : nonvolatile
 Status               : Active
```

3.排错：

如果 snmp 不起作用，需要查看以下几个方面：

1) 交换机上需要配置读写或只读的 community ,例如只读为 pubic ,读写为 private，这两个字符串要与管理站上的管理软件设置一致。
2) 同上述类似的问题，也需要在 snmp 服务器上配置同样的 community，才能够使 snmp 服务器对交换机进行远程察看或者管理。

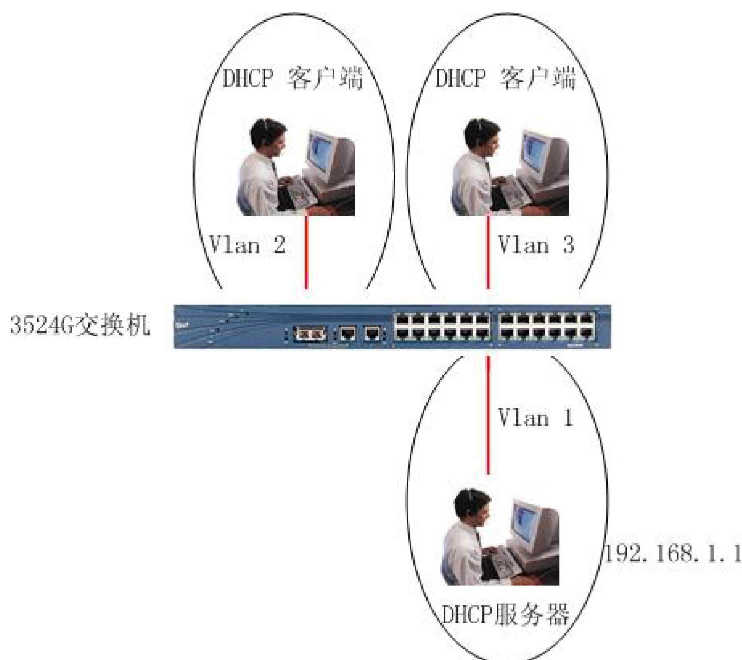
如果交换机不能主动发起 trap 信息给 snmp 服务器，需要查看以下：

1) 需要在交换机上设置 trap 接收者的 ip 地址，也就是 snmp 服务器的 ip 地址。
2) 确保交换机的 ip 地址和 snmp 服务器之间的 ip 是能够相通的。

九． DHCP Relay 配置

1.网络需求：

在 iSpirit3524G 交换机上划分有 3 个 vlan，vlan 1 作为服务器 vlan ，子网 IP 为 192.168.1.0 网段，VLAN2 子网的 IP 网段为 192.168.2.0，VLAN3 子网的 IP 网段为 192.168.3.0，在 VLAN1 内有一台 DHCP 服务器，IP 地址为 192.168.1.1，为其他 VLAN 的 DHCP 客户端提供 IP 地址分配。VLAN2 和 VLAN3 都是用户的使用 VLAN，里面的客户端都使用自动获取 ip 地址。



2.配置步骤：

首先要确保在 35 交换机上配置好了 vlan 和子网，子网之间能够正确进行路由。（关于子网间通信，请查阅子网间通信配置实例一）。然后在 35 交换机上执行：

```
Switch# dhcp server 192.168.1.1       //给交换机指定 dhcp 服务器的 IP 地址
Switch# enable dhcprelay              //打开 dhcprelay 的功能
```

3.排错：

如果在别的 vlan 内的 pc 机不能自动获得 ip 地址，需要从以下几个方面进行检查

1) 确保 dhcp 服务器能正常工作，并且上面已经配置了几个不同子网的 IP 地址池
2) dhcp 服务器在其中的一个 vlan 内，并且和交换机之间的 IP 能正常通信，也能够 ping

通交换机其他几个 vlan 的接口 ip 地址

3) 在交换机上正确配置了 dhcp server 的 IP 地址

通过命令 Switch# show dhcpserver 查看 dhcp server 的 IP 地址是否正确配置了

```
Server Ip Address        : 192.168.1.1
```

4) 查看交换机的 dhcprelay 功能是否打开。

通过在交换机上的命令

```
Switch# show switch
  Ip Address        : 192.168.0.1
  Subnet Mask       : 255.255.255.0
  Default Gateway   : 0.0.0.0
  MAC Address       : 00:09:ca:01:75:02
  BOOTP             : Disable
  DHCP              : Disable
  Spanning Tree     : Enable
  Traffic Classes   : Enable
  IGMP Snooping     : Enable
  Reset             : no reset
  DhcpRelay         : Enable
```

十．802.1x 认证

1.网络需求：

iSpirit 3524G 交换机划分了两个 vlan，vlan 1 是放置了 radius 服务器，ip 网段为 172.16.4.0，子网掩码为 255.255.255.0，iSpirit3524G 上的 vlan1 子网接口 ip 为 172.16.4.1，radius 服务器的 ip 地址为 172.16.4.100。另一个 vlan2 为网络用户使用的 vlan，ip 网段为 172.16.3.0，子网掩码为 255.255.255.0，vlan2 的子网接口为 172.16.3.1，有一用户的 ip 地址为 172.16.3.100 并且联接到 iSpirit3524G 交换机的第 1 端口。为了控制非法用户使用网络，需要在 iSpirit3524 交换机上打开 802.1x 认证机制,在用户使用的 pc 机上安装 802.1x 客户端,用户只有输入正确的用户名和密码并通过 radius 服务器认证，才能访问网络，用户的数据才能被交换机进行路由和转发。

网络拓扑图如下：



2.配置步骤：

2.1 外置 radius 服务器的配置方法

1) 打开 35 的 802.1x 的认证进程

    Switch# dot1x

2) 打开特定端口为 802.1x 的认证端口，本案例为 iSpirit3524G 交换机的 1 端口

    Switch# dot1x control auto 1

3) 为 35 交换机指定 radius 服务器的 ip 地址

    Switch# radius host 172.16.4.100

4) 配置和 radius 服务器相匹配的认证密匙。根据实际情况要和 radius 所配置的一致

    Switch# radius key rad123

5) 查看 802.1x 是否配置正确

```
Switch# show dot1x
Global 802.1X Parameters
Dot1x Status          :    Enable
ReAuth-enabled        :    no
Accounting-enabled    :    yes
ReAuth-period         :    3600
Quiet-period          :    60
Tx-period             :    30
Supp-timeout          :    30
Server-timeout        :    30
Max-req               :    3
reAuthMax             :    3

802.1X Port Summary
PortName    Status       Mode    HostNum
1           Link Up      auto    9
2           Link Down    n/a     9
3           Link Up      n/a     9
```

4	Link Down	n/a	9
5	Link Down	n/a	9
6	Link Down	n/a	9
7	Link Down	n/a	9
8	Link Down	n/a	9

6) 查看 1 端口的状态

Switch# show dot1x 1

Port-control : auto

Maximum hosts : 9

Current Connecting hosts : 0

7) 查看所配置的 radius 服务器是否正确

Switch# show radius-server

PrimaryServerIp : 172.16.4.100

OptionServerIp : 0.0.0.0

UdpPort : 1812

accountingPort : 1813

ShareKey : rad123

Vendor :

NasPort : 0xc353

NasPortType : 0x0f

NasPortServer : 0x02

2.2 内置 radius 服务器的配置方法

1) 配置 3524G 为一台 radius 服务器

Switch# radius host local

2) 添加 radius 服务器的用户名和密码，例子为用户名:test 密码：test

Switch# user add

User Name : test

Password : ****************

Confirm Password : ****************

Deadline : 2111-11-11

please wait!

3) 验证结果：

Switch# show radius-server

PrimaryServerIp : LOCAL

OptionServerIp : 0.0.0.0

UdpPort : 1812

accountingPort : 1813
ShareKey : rad123
Vendor :
NasPort : 0xc353
NasPortType : 0x0f
NasPortServer : 0x02

4) 查看用户
Switch# user show test
userName : =test
password : =test
deadTime : =2111-11-11

其他的配置都一样。

3．排错：

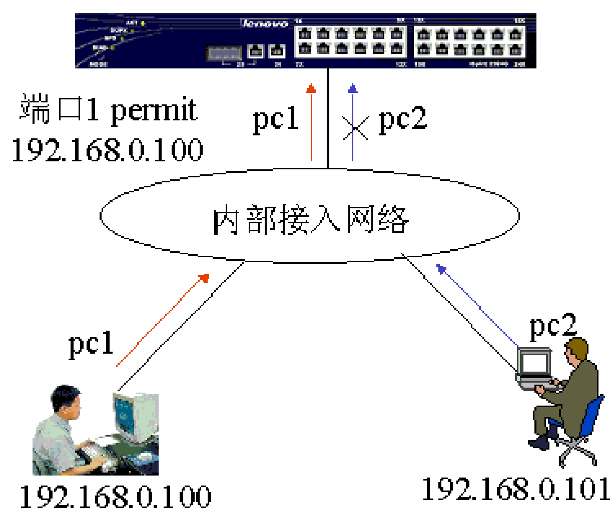
1) 确认一定要打开 802.1x 的认证进程，用 show dot1x 命令
2) 确认打开特定的交换机端口做为认证端口，用 show dot1x 端口号
3) 正确配置 radius 服务器的 ip 地址，用 show radius-server 命令查看
4) 确认 radius 服务器和交换机之间所配置的认证密匙要一致

十一.ACL 访问控制列表配置

1. iSpirit3524G（version 2.2.0 版）

1.1 基于 IP 规则的 ACL

1) 实例：控制交换机端口 1 只能接上 ip 地址为 192.168.0.100 的 pc。如果是其它 ip 地址的 pc 就不能连接到端口 1。也即 ip 地址为 192.168.0.100 的 pc 发出的数据流可以通过交换机的端口 1 转发，而 ip 地址为 192.168.0.101 的 pc 发出的数据流不可以通过交换机的端口 1 转发。



2) 配置：

A ：Switch# access-list 1 permit　host 192.168.0.100

//默认情况下,在上述列表的规则之后隐含了一条规则 deny　any 的规则，此规则是禁止所有。

B:把这标准访问控制列表（access-list 1）应用到 1 端口（对 1 端口流入的数据流做控制）

Switch# port 1

Switch(port 1)#　acl-filter 1

3) 排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表

这条访问控制列表允许源地址为 192.168.0.100 的 IP 数据流通过交换机。用 show access-list 命令列出访问控制列表进行查看。默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

Switch# show acl-filter

ACL group and Port Configuration Information

module/port	groupId	status
1	1	Active

Switch# show access-list 1

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type

SP - Source Port, DP - Destination Port, PT - Protocol Type

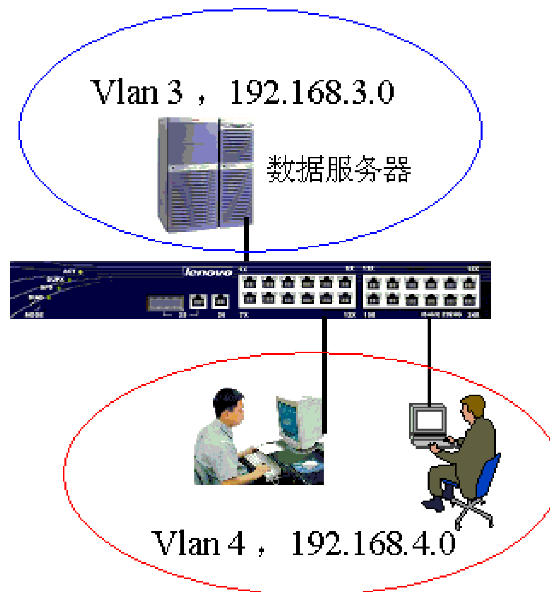
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

Standard IP access list:

GroupId 1 :   reference count(1)

R 1   permit SI 192.168.1.100 Active

1.2 扩展 IP 规则的 acl



1) 在这个网络中，用户都在 172.16.4.0 网段（vlan4），数据库服务器在 172.16.3.0 网段（vlan3），ip 地址为 172.16.3.1。为了保护服务器的安全，不允许其他网段的用户对服务器进行 ping 和 web 服务，而允许其他的服务通过。172.16.4.0 网段为 iSpirit 3524G 的 1 和 2 端口。（在配置 acl 之前，请先确保 vlan3 和 vlan4 能互相通信，具体配置请见 vlan 间通信的配置实例）

2) 配置：

```
Switch# access-list 200 deny icmp any host 172.16.3.1
Switch# access-list 200 deny tcp any host 172.16.3.1 www
Switch# access-list 200 permit ip any any
```

然后把访问控制列表 200 应用到 1 和 2 端口，对流入的数据流做控制

```
Switch# port 1
Switch(port 1)# acl-filter 200
Switch# port 2
```

Switch(port 1)# acl-filter 200

3) 排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表。

对于特定的应用需要指定特定四层网络端口。而且默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

还需要用 show access-list 命令来进行查看访问控制列表配置是否正确

Switch# show acl-filter

ACL group and Port Configuration Information

module/port	groupId	status
1	200	Active
2	200	Active

用 show access-list 命令进行查看

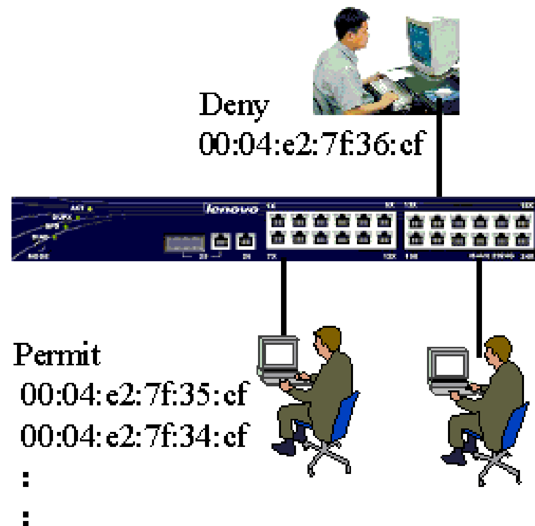
Switch# show access-list 200

```
R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
SP - Source Port, DP - Destination Port, PT - Protocol Type
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

Extended IP access list:
 GroupId 200 : reference count(0)
  R 1 deny icmp SI any DI 172.16.3.1 Active
  R 2 deny tcp SI any DI 172.16.3.1 www Active
  R 3 permit SI any DI any Active
```

1.3 MAC 地址规则的访问控制列表

1)基于安全的考虑，控制特定的 mac 地址为 00:04:e2:7f:36:cf 的特定用户（本例中用户连接到 iSpirit3524G 的 1 端口）的数据流不能通过交换机进行转发，而允许其它 mac 地址的数据流通过。



2) 配置

Switch# access-list 400 deny 0 ip 00:04:e2:7f:36:cf

Switch# access-list 400 permit 0 ip any

然后把访问控制列表应用到 iSpirit3524G 的 1 端口上对流入的数据流做控制

Switch# port 1

Switch(port 1)# acl-filter 400

3) 排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表。还需要用 show access-list 命令来进行查看访问控制列表配置是否正确。

注意 mac 地址一定要书写正确，否则将不起任何作用。而且默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

用来确定访问控制列表的配置正确性

Switch# show acl-filter

ACL group and Port Configuration Information

module/port	groupId	status
1	400	Active

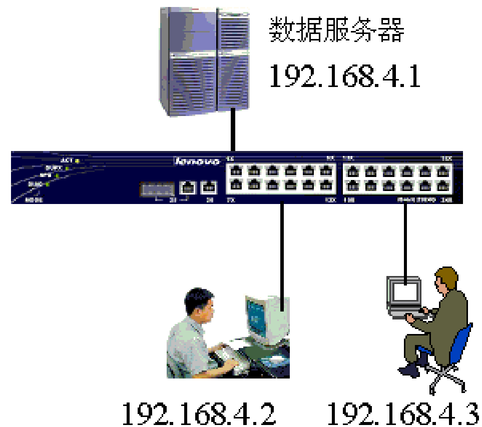
Switch# show access-list 400

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
SP - Source Port, DP - Destination Port, PT - Protocol Type
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

MAC address list:

GroupId 400 : reference count(0)
R 1 deny ip SM 00:04:e2:7f:36:cf DM any Active
R 2 permit ip SM any DM any Active

1.4 单向 ICMP 访问控制列表



1) 为了防止一般用户刺探网络数据服务器，需要一般用户不能够 PING 通数据服务器，但是数据服务器可以 PING 通其他所有用户。这就需要用到 ICMP 协议号。最好的方法是在连接数据服务器的端口上过滤掉由服务器发出的 ICMP 回应包。这就起到了实现 ICMP 单向访问了。数据服务器连接到 iSpirit3524G 交换机的 1 端口

2) 配置

Switch# access-list 300 deny icmp host 172.16.4.1 any echo-reply
Switch# access-list 300 permit ip any any

并且要把这个访问控制列表应用到 1 端口

Switch# port 1
Switch(port 1)# acl-filter 300
Switch# show access-list 300

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
SP - Source Port, DP - Destination Port, PT - Protocol Type
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

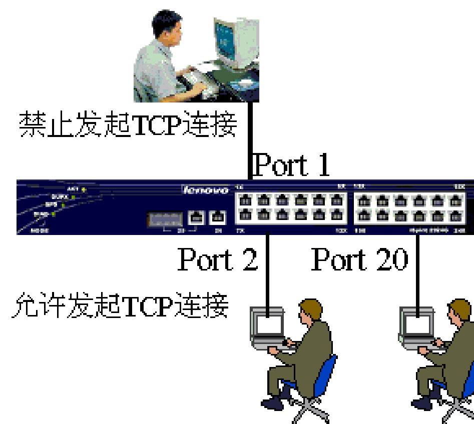
Extended IP access list:
GroupId 300 : reference count(1)
R 1 deny icmp SI 172.16.4.1 DI any echo-reply Active
R 2 permit SI any DI any Active

Switch# show acl-filter

ACL group and Port Configuration Information

port	groupId	status
1	300	Active

1.5 单向 TCP 连接访问控制列表



1) 为了防止一般网络用户主动连接到重要部门的网络，而仅仅允许重要部门可以主动发起到一般网络用户的联接，这就需要用到单向 TCP 连接。最好的方法是在连接一般网络用户的端口上过滤掉由一般用户发起的 TCP 连接。（本案例中，假设一般用户的网络连接到 iSpirit3524G 交换机的 1 端口，重要部门的用户连接到其它端口）

2)配置

```
Switch# access-list 200 deny tcp any any 0 syn 1 ack 0
Switch# access-list 200 permit ip any any
```

并且要把这个访问控制列表应用到 1 端口

```
Switch# port 1
Switch(port 1)# acl-filter 200

Switch# show access-list

 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

 Extended IP access list:
   GroupId 200 : reference count(1)
     R 1 deny tcp SI any DI any syn 1 ack 0 Active
     R 2 permit SI any DI any Active
```

Switch# show acl-filter
ACL group and Port Configuration Information

port	groupId	status
1	200	Active

1.6 基于 acl 规则的带宽限制

网络需求：

限制源地址为 192.168.0.11 的机器以最高 2 M 的流量通。(ip 地址为 192.168.0.11 连接在第 15 端口上)

配置：

1). 配置访问控制列表，并查看结果

```
Switch# access 200 permit ip host 192.168.0.11 any

Switch# show access 200
         R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
         SP - Source Port, DP - Destination Port, PT - Protocol Type
         SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

         Extended IP access list:
           GroupId 200 : reference count(1)
             R 1 permit SI 192.168.0.11 DI any Active
```

2).创建类为 3，并与上述 acl 关联，并查看结果

```
Switch# qos class 3
Switch(class-3)# matc acl 200

Switch# show qos class 3
        classId                :3
        Name                   :
        Status                 :active
        flag                   :Acl    Flag
        valueNumber            :1
        acl group id           :200
        refNumber              :1
```

3).设置策略：

```
Switch# qos pol 2
Switch(policy-2)# class 3
Switch(policy-2-class 3)# meter 2 3

Switch# show qos policy 2
PolicyId               :2
name                   :
node_sum               :1
```

```
refnumber                    :1
Status                       :active

classId                      :3
policy class Status          :active
flag                         :Dscp    Flag
value                        :0
meter                        :used
bandwidth                    :2 (for port 1-24,1 is 1M bit/s;for port 25-26,1
 is 8M bit/s)
burstsize                    :32k bytes
action                       :drop
```

4).应用策略：

```
Switch(port-15)# qos se 2

Switch#   show qos port 15
          port              :15
          flag              :Policy    Flag
          policy id         :2
          Status            :active
```

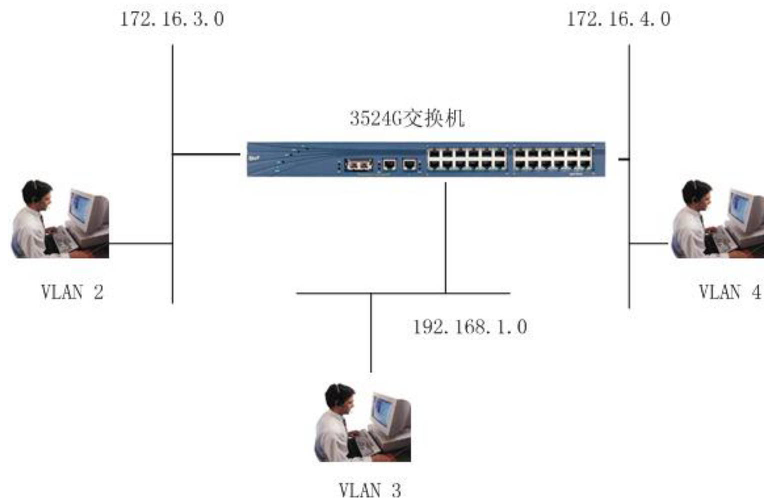
到此，配置完毕。

//**注意：**1.1—1.6 的配置实例是在 iSpirit3524G，软件版本为 2v20 的情况下进行配置的。在命令上与 iSpirit3524G 前期的版本、iSpirit3524F 各个版本有点不同，**设置访问列表之后，要将访问列表应用到端口上。**iSpirit524G 在功能上比 3524F 各个版本都强，主要是增加了访问控制列表的单向控制。以下部分介绍 iSpirit3524G/F(version 2.00 版)的相关配置实例。

2.iSpirit3524G/F（version 2.00 版）

2.1 基于 IP 规则的 ACL

1)一个交换机连接三个子网，设计 ACL，阻塞源地址为 192.168.1.0 网络地址而允许其他网络地址的通信流量通过。



2) Switch# access 1 deny 192.168.1.0 0.0.0.255

3) 排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表

这条访问控制列表阻塞的是源地址为 192.168.1.0 网段的 IP 数据流通过交换机。注意子网反码的写法。用 show access-list 命令列出访问控制列表进行查看，一定要注意源地址和目的地址不要写反。然后进行访问控制列表的查看。

```
Switch# show access-list
  ACL Status      :   Enable
  Standard IP access list:
    GroupId 1 deny srcIp 192.168.1.0 0.0.0.255 any Active
```

2.2 扩展 IP 规则的 acl



1) 在这个网络中，用户都在 172.16.3.0 网段，数据库服务器在 172.16.4.0 网段，ip

地址为 172.16.4.1。为了保护服务器的安全，不允许其他网段的用户对服务器进行 ping 和 web 服务，而允许其他的服务通过。

2) 配置

Switch# access-list 100 deny icmp any host 172.16.4.1

Switch# access-list 101 deny tcp any host 172.16.4.1 www

3) 排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表

对于特定的应用需要指定特定四层网络端口

还需要用 show access-list 命令来进行查看访问控制列表配置是否正确

用 show access-list 命令进行查看

Switch# show access-list

ACL Status : Enable

Extended IP access list:

GroupId 100 deny icmp any destIp 172.16.4.1 Active

GroupId 101 deny tcp any 0 destIp 172.16.4.1 www Active

2.3MAC 地址规则的访问控制列表



1) 基于安全的考虑，控制特定的 mac 地址为 00:04:e2:7f:36:cf 的特定用户的数据流不能通过交换机进行转发。

2)配置

Switch# access-list 700 deny ip 00:04:e2:7f:36:cf

3)排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表

还需要用 show access-list 命令来进行查看访问控制列表配置是否正确

注意 mac 地址一定要书写正确，否则将不起任何作用

用来确定访问控制列表的配置正确性

```
Switch# show access-list
  ACL Status      :   Enable
  MAC address list:
    GroupId 700 deny ip srcMac 00:04:e2:7f:36:cf Active
```

2.4 基于 vlan 规则的 acl



1) 禁止转发 VLAN3 的所有用户数据
2) 配置

```
Switch# access-list vlan 3 deny
```

3) 排错

```
Switch# show access-list
  ACL Status      :   Enable
  Vlan list:
    VlanId 3 deny Active
```

2.5 基于 acl 规则的带宽限制

1) 对一个特定的端口 1 的流入数据流量做 1M 带宽的限制。

```
Switch# access-list port 1 all in permit 1
Switch# show access-list
  ACL Status      :   Enable

  Port list:
    Port 1 permit ingress 1*125kByte/s Active
```

2) 基于特定访问控制列表的带宽限制

限制源地址为 192.168.1.0 网段的机器以最高 10M 的流量通过交换机
先建立一个标准访问控制列表，以允许 192.168.1.0 网段的设备流量通过交换机
Switch# access-list 1 permit 192.168.1.0

然后对这条访问控制列表进行 10M 的带宽控制，
Switch# access-list rate-limit 1 10

通过 show 命令进行带宽配置查看

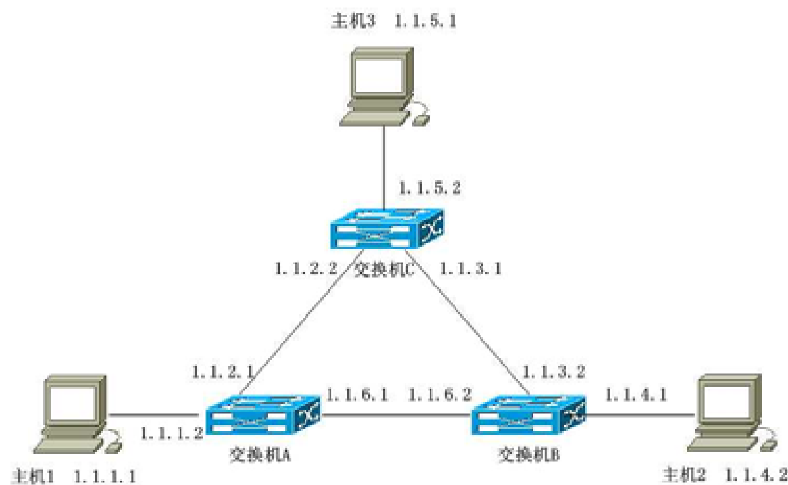
```
Switch# show access-list 1
 ACL Status       :    Enable

 Standard IP access list:
  GroupId 1 permit srcIp 192.168.1.0 any 10*125kByte/s Active
```

十二.静态路由

1.网络需求：

如下拓扑图所示，要实现整个网络不同网段都可以相互通信。为了实现不同网段的通信，有一种简单的方法就是通过配置静态路由来实现。



2.配置步骤：

1) 在每台交换机上配置三个网段（三个子网），并保证子网间可以相互通信。接着就开始配置静态路由。

2)配置各交换机的静态路由

！配置三层交换机A 的静态路由

```
Switch(route-config)# ip static route
Dest Ip: 1.1.4.0
Net Mask: 255.255.255.0
gate way: 1.1.6.2
Static Route Name:a12
Use HareWare(y/n)y
```

——————————————————————————————

```
Switch(route-config)# ip static route
Dest Ip: 1.1.5.0
Net Mask: 255.255.255.0
gate way: 1.1.2.2
Static Route Name:a13
Use HareWare(y/n)y
```

！配置三层交换机B 的静态路由

```
Switch(route-config)# ip static route
Dest Ip: 1.1.5.0
Net Mask: 255.255.255.0
gate way: 1.1.3.1
Static Route Name:a23
Use HareWare(y/n)y
```

——————————————————————————————

```
Switch(route-config)# ip static route
Dest Ip: 1.1.1.0
Net Mask: 255.255.255.0
gate way: 1.1.6.1
Static Route Name:a21
Use HareWare(y/n)y
```

```
！配置三层交换机C 的静态路由
Switch(route-config)# ip static route
Dest Ip: 1.1.1.0
Net Mask: 255.255.255.0
gate way: 1.1.2.1
Static Route Name:a32
Use HareWare(y/n)y
__________________________________________
Switch(route-config)# ip static route
Dest Ip: 1.1.4.0
Net Mask: 255.255.255.0
gate way: 1.1.3.2
Static Route Name:a31
Use HareWare(y/n)y
```

3.排错：

如果接口的物理状态和链路层协议状态均已处于 UP，但 IP 报文不能正常转发。处理方法如下：

- 用 **show ip static route table** 命令查看是否正确配置相应静态路由。
- 用 **show ip route table** 命令查看该静态路由是否已经生效。
- 查看是否在接口上未指定下一跳地址或下一跳地址不正确。
- 查看是否能够连通下一跳。
- 查看指定的发送数据包的主机的指定网关是否正确。

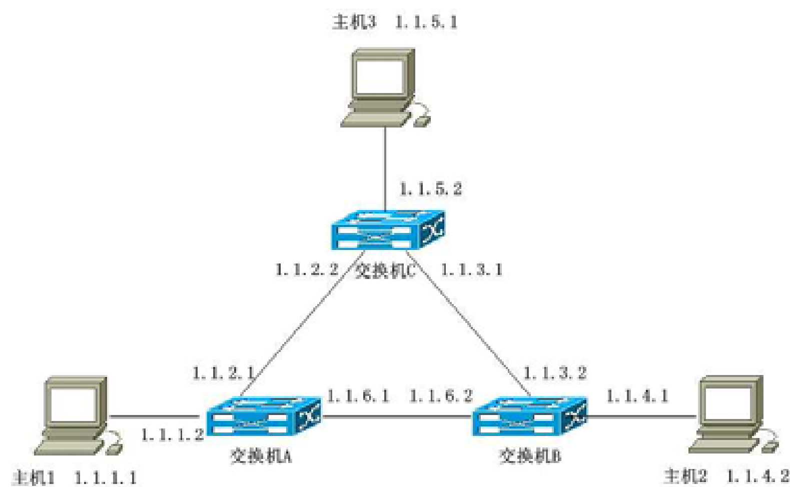
十四.ip 配置

1.实例一

1.1 网络需求：

三台交换机两两相连，分别有6个网段，都启用rip协议，实现三台PC机之间能够两两互通。

网络拓扑图：



1.2 配置步骤：

在每台交换上配置 **Switch (route_config)# ip route protocol rip**

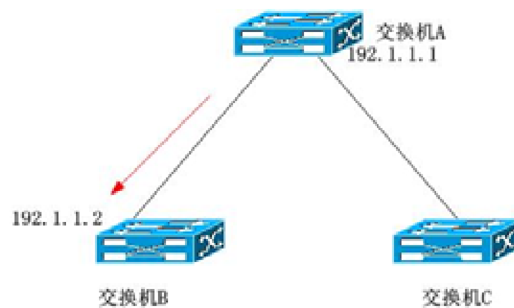
启用rip 协议（默认情况下rip协议是关闭的）

2.实例二

2.1 网络需求

三层交换机A 与B， A 与C 分别相连，若交换机A（192.1.1.1）只想把路由更新信息发送到相邻交换机B（ 192.1.1.2）而不发给相邻路由器C。

拓扑图如下：



2.2 配置步骤

1) 进入交换机 A 的路由模式

2）设置交换机 A 某一接口的发送类型为“ nosend”

Switch(rip_config)# send type

Interface Ip address:192.1.1.1

Send Type:nosend

附件：配置超级终端

1) 将交换机背后的串口与计算机的串口（com1/com2）用串口线连接起来。
2) 打开计算机按照图 1 打开超级终端

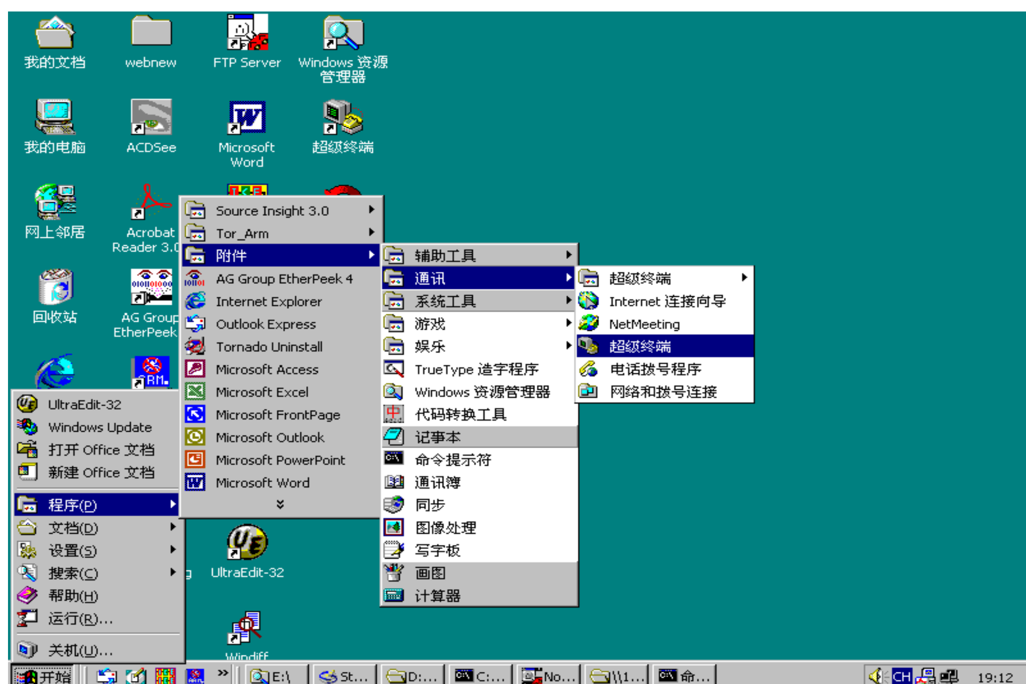


图 1 打开超级终端

3) 按图 2，3， 4 配置超级终端



图 2

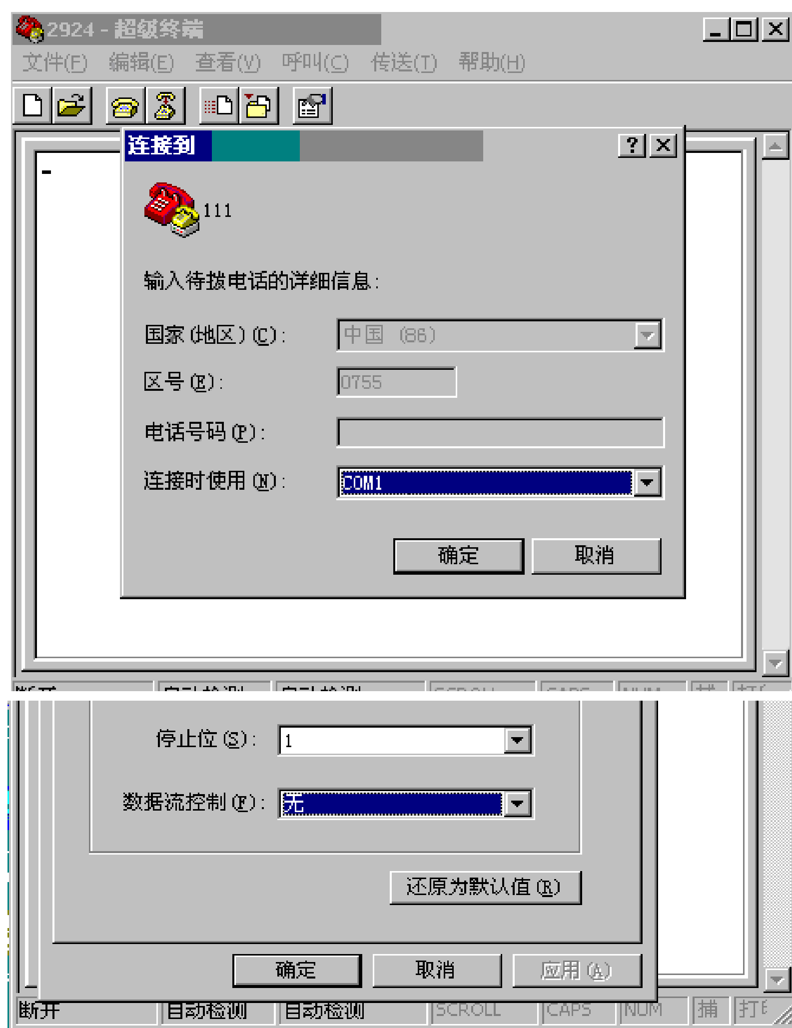


图 3

图 4

4) 点击确定，就可以连接到交换机的 CLI 管理界面。